УДК 004.056.55

РОЗПОДІЛ ЙМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛІВ ЗА МОДУЛЬНИМ ДОДАВАННЯМ У БЛОКОВИХ ШИФРАХ ІЗ ФІКСОВАНИМИ КЛЮЧАМИ

В. Ю. Бахтігозін[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У данній роботі наводяться розподіли ймовірностей диференціалів та диференціальних характеристик відносно операції додавання за модулем 2^n у блокових шифрах із фіксованим ключем.

Ключові слова: диференціальний криптоаналіз, розподіл диференціалів, блокові шифри

Вступ

Диференціальний криптоаналіз є одним з найпотужніших методів криптоаналізу симетричних блокових шифрів. Сучасні методи доведення стійкості алгоритмів шифрування до диференціального криптоаналізу фактично зводять відповідні оцінки стійкості до певних обчислювальних параметрів раундових перетворень та їх окремих компонент, таких як S-блоки (див., наприклад, [1, 2, 3, 4]). Зазвичай для підвищення стійкості до даного методу аналізу у блокових шифрах обираються бієктивні S-блоки (тобто підстановки на бітових векторах) із мінімально можливими імовірностями диференціалів.

Далі будуть розглянуті розподіли характеристик та диференціалів для ітеративних шифрів, ключ в котрих вводиться за модульним додаванням.

1. Необхідні терміни та позначення

Диференціалом перестановки π називається пара (a, b), яка трактується як різниці на вході та на виході

$$(u - v) \bmod 2^n = a, (\pi(u) - \pi(v)) \bmod 2^n = b$$

де $a, b \in (Z_{2^n}, +)$, n – розмір перестановки.

Ймовірністю диференціала називається величина

$$DP(a, b) = Pr\{\pi(x + a) - \pi(x) = b\}$$

де віднімання і додавання відбуваються за модулем $2^n, x \in Z_{2^n}$.

Під потужністю диференціала будемо розуміти

$$N(a, b) = 2^n \cdot DP(a, b)$$

З [5] відомо, що для $ord(a), ord(b) \neq 2$ потужність має розподіл Пуассона з параметром 1

$$N(a, b) \sim Poi(1)$$

Вагою диференціала називається

$$w_d(a, b) = -\log_2 DP(a, b)$$

Далі будуть розглядатись нетривіальні диференціали, тобто $a, b \neq 0$.

Більшість блокових шифрів побудовані як послідовність раундів, де кожен раунд – це залежне від ключа перетворення. Ключі, які використовуються в одному з цих перетворень, називаються раундовими ключами. Раундовий ключ утворюється з ключа шифрування за допомогою ключового розкладу. Вважаємо, що n – розмір блоку шифру, h – розмір ключа, r – кількість раундів.

Шифрами зі змінним ключем будемо називати шифри, в яких раунд складається з деякої перестановки, незалежної від ключа. Ключ вводиться між раундами, за допомогою простої операції – в даному випадку, додавання за модулем.

$$Y = X_r + k_r, X_i = \rho(X_{i-1} + k_{i-1}), i = \overline{(0, r-1)}$$

де Y – шифртекст, X_0 – відкритий текст, k_i – раундові ключі.

Шифр з довгим ключем – шифр зі змінним ключем з простим ключовим розкладом. В цьому випадку $h = n(r + 1)$, ключ шифрування є конкатенацією всіх раундових ключів. Далірозглядаємо такі шифри з довгим ключем, які є марковськими шифрами.[6]

Характеристикою Q над r-раундовим шифром називається послідовність різниць

$$Q = (q^{(0)}, q^{(1)}, q^{(2)}, ..., q^{(r)})$$

Потужність характеристики для фіксованого ключа визначається так само як і потужність диференціалу

$$N[k](Q) = |\{(u, v) : u - v = q^{(0)}, \rho(u) - \rho(v) = q^{(1)}...\}|$$

де ρ – раундове перетворення.

2. Розподіл ймовірностей диференціалів у шифрах зі змінним ключем

Середнім DP характеристики в шифрі з довгим ключем називається $DP(Q) = \prod DP(q^{(j-1)}, q^{(j)})$. [6]

Позначимо через $Q_{(a,b)}$ множину вкладених характеристик між різницями a та b, тобто $q^{(0)} = a, q^{(r)} = b$. Тоді потужність диференціалу (a, b) дорівнює

$$N[k](a,b) = \sum_{Q_{(a,b)}} N[k](Q_{(a,b)})$$

де $N[k](a,b)$ та $N[k](Q_{(a,b)})$ відповідні потужності при фіксованому ключі. Звідси повна потужність диференціалу (a, b) ітеративного шифру

$$N_{tot}(a,b) = \sum_k N[k](a,b) = \sum_k \sum_{Q_{(a,b)}} N[k](Q_{(a,b)}) = \sum_{Q_{(a,b)}} N_{tot}(Q_{(a,b)})$$

Визначимо шифр з довгим ключем асоційований з шифром зі змінним ключем, замінивши його ключовий розклад на тривіальний. Таким чином множина 2^h розширених ключових значень, отриманих за допомогою ключового розкладу є підмножиною $2^{n(r+1)}$ ключів шифру з довгим ключем. Для певного шифру з довгим ключем повна потужність усіх характеристик і диференціалів величина детермінована і легко обчислюється. Розподіли середніх та з фіксованим ключем потужностей характеристик та диференціалів у шифрі зі змінним ключем визначається відповідними розподілами в асоційованому шифрі з довгим ключем. Очікуваною ймовірністю диференціалу або характеристики (EDP) у шифрі зі змінним ключем називається відповідне середнє DP у шифрі довгим ключем.[6]

Розглянемо асоційований шифр з довгим ключем. $2^{n(r+2)}$ вхідних пар рівномірно розподілені між ключами: 2^n входів на кожен ключ. Для кожної характеристики Q, множина входів, що належать цій характеристиці для фіксованого ключа можна змоделювати як вибірку із популяції. Далі популяцією будемо називати всі входи (для всіх ключів) в шифрі з довгим ключем, на відміну від вибірки – входи для фіксованого ключа. [6]

- Загальний розмір популяції – кількість усіх входів, $2^{n(r+2)}$
- Кількість успіхів у виборці – кількість входів, що слідують характеристиці, $2^{n(r+2)-z}$. $z = w_d(Q), EDP(Q) = 2^{-z}$
- Розмір вибірки – кількість входів для фіксованого ключа, 2^n

Звідси за [7] маємо гіпергеометричний розподіл

$$Pr(N[k](Q) = i) = \frac{C^i_{2^{n(r+2)-z}} C^{2^n - i}_{2^{n(r+2)} - 2^{n(r+2)-z}}}{C^{2^n}_{2^{n(r+2)}}}$$

Гіпергеометричний розподіл апроксимується біноміальним розподілом з параметрами 2^n та 2^{-z}, який у свою чергу – розподілом Пуассона з параметром $\lambda = 2^{n-z}$.

Потужність диференціалу (a, b) при фіксованому ключі це сума потужностей всіх відповідних характеристик. Тому

$$N[k](a,b) \sim Poi(\sum_{Q_{(a,b)}} 2^{n - w_d(Q_{(a,b)})})$$

Повна потужність характеристики дорівнює сумі потужностей по всім 2^h значенням ключа. Якщо $h \ll n(r+1)$, то потужності з фіксованими ключами можна вважати незалежними величинами. Отже

$$N_{tot}(Q) \sim Poi(2^{h+n-z})$$

З цього випливає, що повна потужність диференціалу

$$N_{tot}(a,b) \sim Poi(2^{h+n} EDP(a,b))$$

Більшість диференціальних характеристик та диференціалів мають EDP значно більше ніж 2^{-h-n}.[6] Тому, в шифрах зі змінним ключем, середнє DP диференціальної характеристики або диференціала це випадкова величина з розподілом, близьким до нормального з середнім EDP та дисперсією $2^{-h-n} \cdot EDP$. Розглянуті функції розподілу дають ймовірності для всіх можливих ключових розкладів.

Висновки

У даній роботі було розглянуто розподіли ймовірностей диференціальних характеристик та диференціалів за модульним додаванням у ітеративних блокових шифрах. Було встановлено, що ймовірності диференціалів блокових шифрів із фіксованими ключами асимптотично підкорюються розподілу Пуассона, параметром якого виступають середні за ключами імовірності

Перелік використаних джерел

1. Nyberg K., Krudsen L. R. Provable Security Against a Differential Attack // Journal of Cryptology. — 1995. — no. 1.
2. C. Adams St. Travares. Designing S-boxes resistant to defferential cryptanalysis. — URL: `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.2536`.
3. Park S. On the security of Rijndael-like structures against differential and linear cryptanalysis / S. Park, S .H. Sung, S. Chee et al. // Advances in Cryptology. — 2002. — P. 176–191.
4. On the security of Rijndael-like structures against differential and linear cryptanalysis / S. Park, S .H. Sung, S. Lee, J. Lim // Fast Software Encyprion. — 2003. — P. 247–260.
5. Hawkes P. M., O'Connor L. J. XOR and NON-XOR Differential Probabilities // Advances in Cryptology. — 1999.
6. Daemen J., Rijmen V. Probability distributions of Correlation and Differentials in Block Ciphers // Journal of Mathematical Cryptology. — 2005.
7. Feller W. An Introduction to Probability Theory and Its Applications. — Wiley & Sons, 1968.